Complete Listing of Claims

Claims:

1. **(currently amended)** In a ~~computer--system~~ **computing device,** a method for secure communication, comprising:

using a single secure communication port for secured communications between a server and a client, and between two clients, for ease of access and transparency, from any location to any location, within said ~~computer---system~~ **computing device**;

requesting communication by a client for connection to a communication server;

receiving said communication request and a handshake sequence is performed between said client and said communication server;

establishing a secure connection between said client and said communication server;

coordinating a new connection with a second client by the communication server; and

establishing a connection between the two clients via the communication server wherein said single communication port allows access from behind network securing means by establishing a secure proxy communication between said two clients by utilizing end-to-end secured data transfer.

2.**(currently amended)** The method of claim 1, wherein said single secure communication port is SSL port 443 **[[.]]or any other port, allowing secure communication using SSL or any other protocol.**

3.**(currently amended)** The method of claim 1, wherein **use of** said single communication port allows access from behind **network securing means such as** firewalls **or network address translation means** by establishing a secure proxy ~~communication~~ **connection** between said two clients **[[.]] using a communication server as a traffic controller.**

4.**(currently amended)** The method of claim 1, wherein **use of** said single communication port allows access inside

4. **(currently amended)** The method of claim 1, wherein **use of** said single communication port allows access inside firewalls by establishing a secure proxy connection between said two clients **[[.]]** **using said communication server to enable said secure proxy connection to securely transfer end-to end secured communications.**

5. **(currently amended)** The method of claim 1, wherein **use of** said single communication port allows ease of management **of communications** by establishing a secure **proxy** connection between said two clients **[[.]]** **supporting multiple application protocols**.

6. **(currently amended)** The method of claim 1, wherein **use of** said single communication port allows the elimination of a need to change firewall configurations by establishing a secure proxy communication between said two clients **[[.]]** **utilizing encrypted end-to end data transfer that does not have to be decrypted at said communication server.**

7. **(currently amended)** A method for secure communication in a computer network, comprising:

using a single secured communication port for secured communications within said computer network, for establishing

secured communication between two or more clients via a communication proxy server [[.]] ;

requesting communication by a client for connection to a communication server;

receiving said communication request and a handshake sequence is performed between said client and said communication server;

establishing a secure connection between said client and said communication server;

coordinating a new connection with a second client by the communication server; and

establishing a connection between the two clients via the communication server wherein said single communication port allows access from behind network securing means by establishing a secure proxy communication between said two clients by utilizing end-to-end encrypted data transfer.

8. **(currently amended)** The method of claim 7 **[[8]]**, wherein said single secured communication port is SSL port 443 **[[.]]** **or any other port.**

9. **(currently amended)** A method for secure communication in a computer system, comprising the steps of:

using a single secure communication port;

requesting communication by a client for connection to a communication server;

receiving said connection request and a handshake sequence is performed between said client and said communication server;

establishing a secure connection between said client and said communication server;

coordinating a new connection with **[[the]]** **a second** client by the communication server;

initiating a handshake sequence with a second client via the communication server; and

establishing a connection between the two clients via the communication server **wherein said single communication**

port allows access from behind network securing means by establishing a secure proxy communication between said two clients by utilizing end-to-end secured data transfer.

.

10.**(currently amended)** The method of claim 9, wherein said single connection port is SSL port 443 **[[.]]** **or any other port.**

11.**(currently amended)** The method of claim 9, wherein a single communication protocol using said single secure port is **utilized** **[[used]].**

12.**(currently amended)** The method of claim 9, wherein multiple protocols using said single secure communication port are **utilized** **[[used]].**

13. **(currently amended)** The method of claim **9** **[[11]]**, wherein **use of** said single secure communication port allows access from behind **network securing means such as** firewalls or **network address translation means** by establishing a secure proxy connection between two clients **[[.]]** **using a communication server as a traffic controller.**

.

14. **(currently amended)** The method of claim **9** **[[11]]** , wherein **use of** said single secure communication port allows access inside firewalls by establishing a secure proxy connection between two clients **[[.]]** **using said communication server to enable said secure proxy connection to securely transfer end-to end secured communications.**.

15. (**currently amended)** The method of claim **9** **[[11]]** , wherein **use of** said single secure communication port allows ease of management by establishing a secure proxy connection between two clients **[[.]]** **using said communication server to enable said secure proxy connection to securely transfer end-to end encrypted communications.**.

16. **(currently amended)** The method of claim **9** **[[11]]** , wherein **use of** said single secure communication port eliminates the need to change firewall configuration by establishing a secure proxy connection between two clients **[[.]]** **utilizing secured end-to end data transfer that does not have to be decrypted at said communication server**.

17.(currently amended) **A computer-readable medium encoded with a computer program** ~~Computer--software~~ for **[[a]]** secure communication in a computer system, comprises:

means for using a single secure communication port for secured communication within said computer system for establishing secured communications between two or more clients **[[.]]**;

requesting communication by a client for connection to a communication server;

receiving said communication request and a handshake sequence is performed between said client and said communication server;

establishing a secure connection between said client and said communication server;

coordinating a new connection with a second client by the communication server; and

establishing a connection between the two clients via the communication server wherein said single communication port allows access from behind network

securing means by establishing a secure proxy communication between said two clients by utilizing end-to-end secured data transfer that does not require decryption at said communication server.

18. **(currently amended)** The **computer-readable medium encoded with a computer program)** ~~computer software~~ of claim 17, wherein said single secure port is SSL port 443 **[[.]]** **or any other port.**